REMARKS

The non-final Office Action dated 7 July 2006 has been received and its contents carefully studied. Claims 1-65 are pending, and all stand rejected. The independent claims are claims 1, 29, 30, 58, 59, 60, and 65.

The Office Action says at page 2, paragraph 3 that all of the claims 1-65 are now rejected as anticipated under 35 USC § 102(b) by *Hayashi Seiichiro* (JP 09-261218). However, Applicant assumes that this is a mistake, and that only claims 1-23, 26-52, and 55-56 were meant to be rejected as anticipated by *Seiichiro*. After all, page 7 of the Office Action says that claims 24-25 and 53-54 are rejected as obvious from *Seiichiro* in view of *Hurtado*. Claims 24-25 and 53-54 are not mentioned on pages 3-6 of the Office Action. Applicant therefore respectfully requests clarification as to whether the Office Action meant to say on page 2, paragraph 3 that claims 24-25 and 53-54 are rejected as anticipated under 35 USC § 102(b) by *Seiichiro*.

The *Seiichiro* reference was not previously cited during prosecution of the present application. Applicant does not see anything in *Seiichiro* regarding usage limitations, which is the subject of claims 24-25 and 53-54. As the Office Action says at page 7, "*Seiichiro* fails to disclose usage limitations." Therefore, Applicant does not understand why it is stated at page 2, paragraph 3 that, "Claims 1-65 are rejected under 35 U.S.C. 102(b) as being anticipated by Hayashi Seiichiro JP 09-261218."

Summary of the Present Invention

The present invention includes a method allowing user identification or data encryption with a public key technique, for a user who already has a certificate and corresponding secret key for signatures using another system. For example, a temporary key can be used by

allowing the user to create acceptable certificates for those temporary keys. According to other (e.g. prior art) methods, such user-created certificates are not considered valid. In an embodiment of the present invention, user-created certificates are accepted, but they use the identity from a certificate already provided by a certificate authority (CA).

The Present Amendments

The claims are now amended without prejudice, in order to expedite allowance. All of the independent claims are now amended to include the limitations of claim 24 regarding usage limitations. The independent claims are further amended to require that one of the usage limitations is a temporal limitation, as described on page 13 of the application as originally filed. That page of the application also describes the purpose of the temporal limit (i.e. to limit the chance that a user-generate certificate will be used fraudulently). The amendments of the independent claims are further supported by the last full paragraph on page 4 of the application as originally filed.

Various other minor formatting amendments are made as well (e.g. deleting acronymns). Claim 65 is merely amended to more closely conform to claim 29. New claim 66 is a rephrased version of claim 60. New claim 67 is a rephrased version of claim 61.

The Present Amended Independent Claims Are Note Obvious From The References

The claims as amended are not obvious from *Seiichiro* in view of *Hurtado*. There is no suggestion at all in *Seiichiro* that the method disclosed there will potentially lead to increased fraud. In contrast, the present application recognizes that problem at page 13, and the solution is to place an appropriate temporal limit on the usage of the certificate, which is now claimed in claim 1. Claim 1 further specifies that the temporal limit on usage is such that once a session on the second system is completed, then the certificate or a corresponding key is destroyed. Because the cited references nowhere suggest that the method will result in

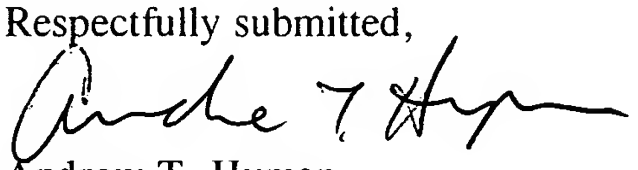
increased risk of fraud, there is no motivation to counteract that risk as described in both amended claim 1 and the other independent claims.

Hurtado does disclose a temporal usage limitation at column 9, lines 61-62. However, there is no suggestion in *Hurtado* that such a temporal limitation will be designed to counteract an increase fraud risk resulting from *Seiichiro*, and much less does *Hurtado* suggest that the appropriate temporal limitation will be such the certificate or a corresponding key is destroyed, that once a session on the second system is completed, as is now claimed in claim 1 and the other independent claims.

Conclusion

It is therefore respectfully submitted that claims 1-67, as presently amended, are distinguished over the cited art and that the claims are therefore in condition for allowance. Such action is earnestly solicited.

Respectfully submitted,



Andrew T. Hyman
Attorney for the Applicant
Registration No. 45,858

ATH/mbh
WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, PO Box 224
Monroe CT 06468
(203) 261-1234